



IsarFlow Whitepaper

Effiziente Verfolgung von Last- und Fehlersituationen im Netz mit IsarFlow

Einführung

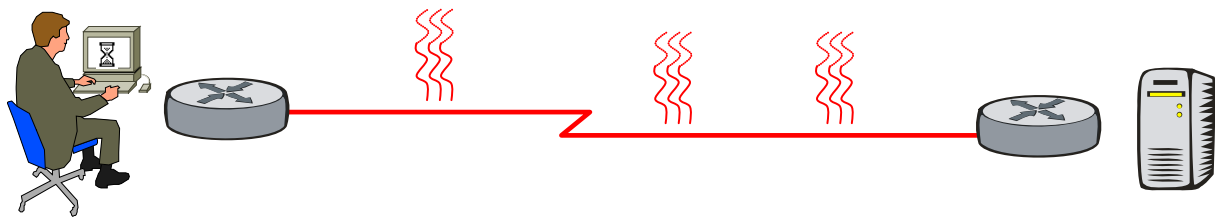
Im laufenden Betrieb eines Netzes bilden die genauen Kenntnisse über die vorhandenen Verkehrsmuster eine essentielle Basis für ein effizientes Arbeiten. Neben einer reinen Auslastung ist es wichtig zu wissen, welche Protokolle zu einem bestimmten Zeitpunkt das Netz belasteten, um nachträglich eventuelle Performanceprobleme zu analysieren. Die genaue Kenntnis darüber, welche Endgeräte oder Sessions den Hauptanteil der Netzauslastung tragen, hilft wertvolle Zeit sparen wenn es zu Antwortzeitproblemen im Netz kommt.

In den vorliegenden Beispielen wird beispielhaft aufgezeigt, wie Fehler- oder Lastsituationen nachverfolgt werden können und somit Maßnahmen für einen reibungslosen Netzbetrieb definiert werden können.

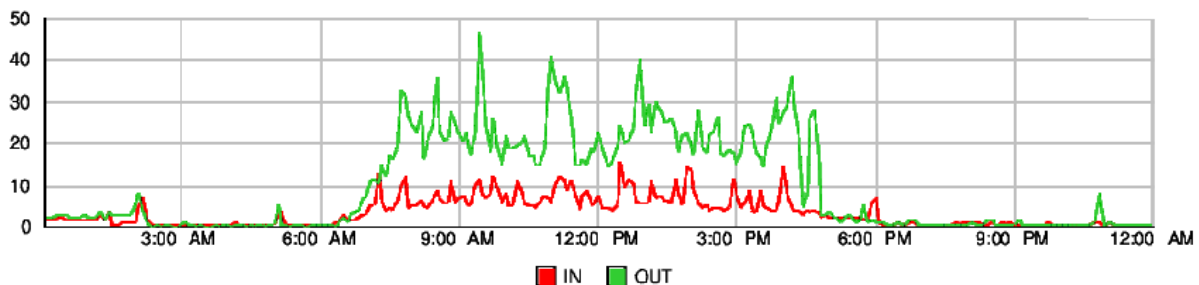


Anwendungsfall #1 – Auslastung von WAN-Leitungen

Kleinere Aussenstellen werden in der Regel mit relativ geringen Bandbreiten an zentrale Standorte angebunden. Häufig kommt es vor, dass Verkehr über diese Leitungen nicht mit der erwarteten Performance übertragen wird.



Klassische SNMP Netzwerk-Management Tools zeigen zwar an, inwieweit einzelne Leitungen (incoming/outgoing) zu einem bestimmten Zeitpunkt ausgelastet sind, bei der Bestimmung der Verursacher kommt man mit SNMP jedoch nicht weiter :

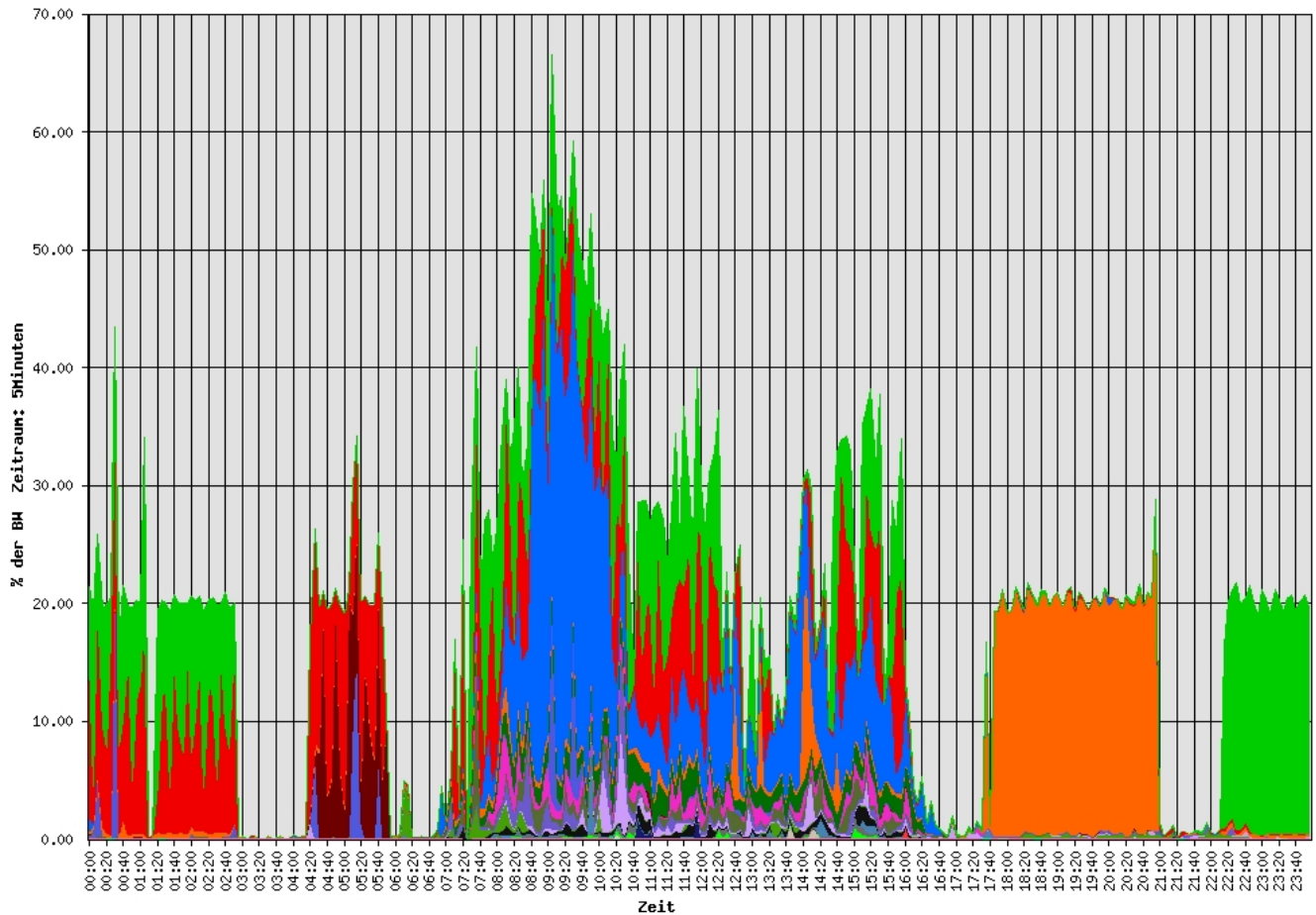


Im Gegensatz zu SNMP werden bei Netflow basierten Analysen nicht einzelne Parameter (wie Interface Input/Output, CPU, Memory, etc...), sondern session-orientierte Variablen erfasst. D.h. eine Beschreibung der Eigenschaften einer Session. Dies bietet z.B. die Möglichkeit, bei Analysen von Datenströmen über ein ausgewähltes Interface nicht nur die Protokoll-Zusammensetzung dieses Verkehrs, sondern auch die zugehörigen Verursacher (IP-Adressen) einfach herauszufinden. Hierfür gibt es in IsarFlow die beiden Analysen ‚Intraday‘ und ‚Top Sessions‘ (oder die Analyse ‚MaxTraffic‘ für die Top Talker).



Intraday Analyse

View: Link to Amsterdam
Bandbreite: 1.985 Mbps (full duplex)
04.01.2007 00:00 - 23:55
(Intervall 5 min)



Nr.	Protokoll	Byte	%
1	AppNo5.2066-3027	1.89 GB	24.28
2	AppNo2.3664-5059	1.67 GB	21.36
3	HTTP-PROXY_8080	1.54 GB	19.70
4	AppNo31.1029-1233	1.30 GB	16.70
5	SAP.3263.TCP	246.98 MB	3.09
6	TCP-OTHER	246.71 MB	3.09
7	FTP-DATA.tcp.20	172.77 MB	2.16
8	SAP.3500.TCP	159.61 MB	2.00
9	HTTP.tcp.80	151.15 MB	1.89
10	AppNo1.1235-1432	116.12 MB	1.45
11	SMTP.tcp.25	100.47 MB	1.26
12	MICROSOFT-DS.tcp.445	68.44 MB	0.86
13	SAP.3201.TCP	60.78 MB	0.76
14	PRINTER.tcp.515	34.97 MB	0.44
15	SAP.3366.TCP	17.70 MB	0.22
16	SAP.3266.TCP	12.70 MB	0.16
17	VNC.tcp.5901	8.25 MB	0.10
18	W2K-AD.1027.TCP	7.71 MB	0.10
19	LDAP.tcp.389	4.44 MB	0.06
20	SAP.3389.TCP	4.17 MB	0.05
21	NETBIOS-SSN.tcp.139	2.56 MB	0.03
22	SAP.3262.TCP	2.47 MB	0.03
23	KERBEROS.udp.88	1.80 MB	0.02
24	ICMP	1.66 MB	0.02
25	HTTPS.tcp.443	1.22 MB	0.02
dargestellte Elemente		7.79 GB	99.85
Summe		7.80 GB	100.00
CSV Export			



Über die Top Session Analyse findet man heraus welche IP-Adressen für einen bestimmten Anwendungs-Verkehr verantwortlich waren :

Top Sessions

View: Link to Amsterdam
04.01.2007 08:30 - 10:20

<u>Nr.</u>	<u>Source</u>	<u>Destination</u>	<u>Protokoll</u>	<u>Byte</u>	<u>Prozent des gesamten Traffic</u>
1	192.109.121.69	10.8.1.10	HTTP-PROXY_8080	558.40 MB	35.91
2	10.8.2.10	10.10.9.46	AppNo2.3664-5059	203.80 MB	13.11
3	10.10.9.46	10.8.2.10	AppNo5.2066-3027	199.21 MB	12.81
4	10.8.1.10	10.10.2.14	HTTP-PROXY_8080	173.80 MB	11.18
5	10.250.8.2	10.8.2.12	FTP-DATA.tcp.20	47.66 MB	3.07
6	10.8.1.10	192.109.121.69	HTTP-PROXY_8080	33.39 MB	2.15
7	10.8.2.15	62.134.52.2	SMTP.tcp.25	18.24 MB	1.17
8	10.8.1.10	10.10.9.109	HTTP-PROXY_8080	16.32 MB	1.05
9	10.8.2.15	10.10.9.118	AppNo1.1235-1432	13.22 MB	0.85
10	10.250.8.112	10.8.2.10	PRINTER.tcp.515	12.39 MB	0.80
Summe				1.25 GB	82.10%
Gesamter Traffic				1.52 GB	100.00%
CSV Export					



Anwendungsfall #2 – schneller Überblick zu Fehler-Situationen

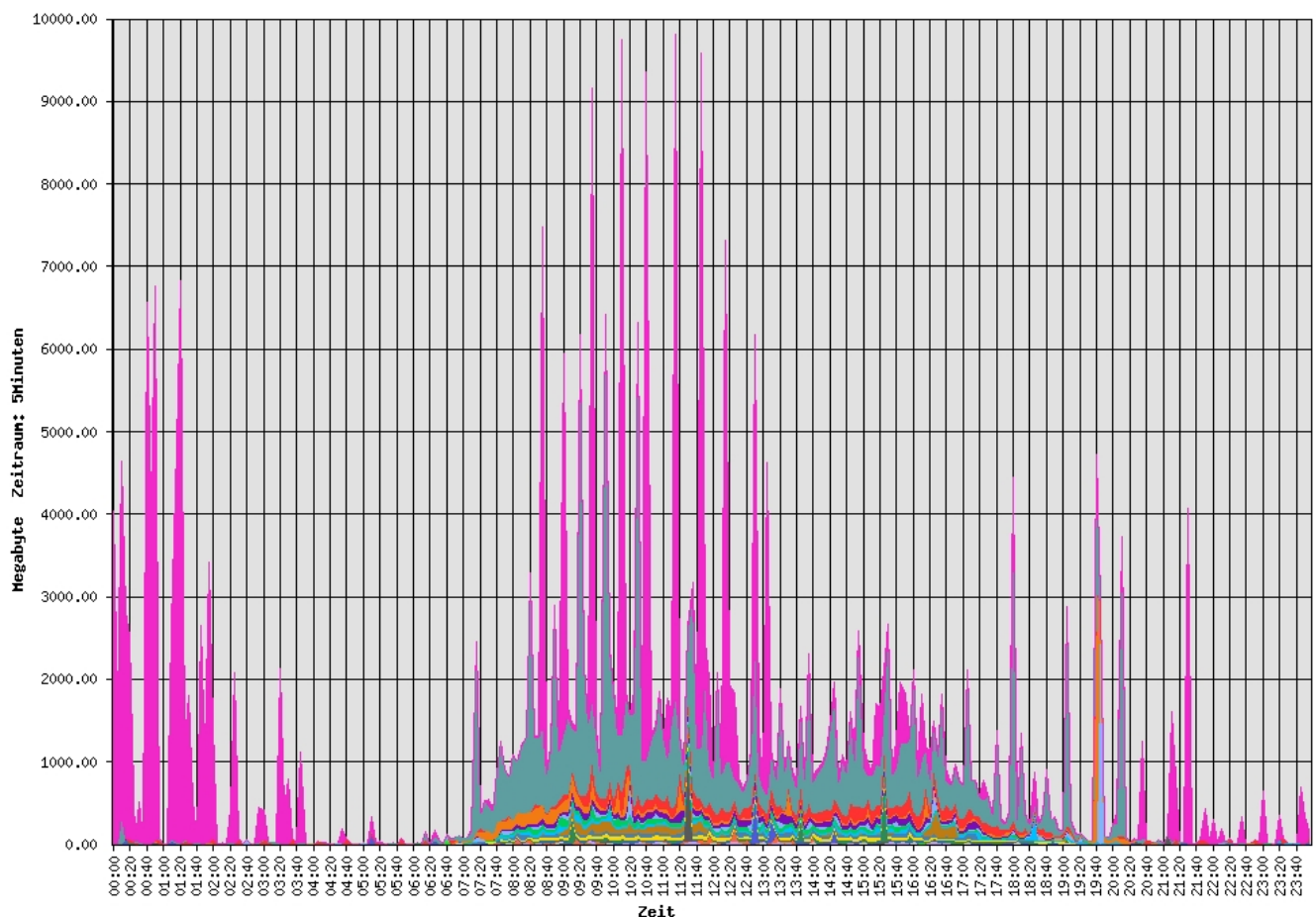
Durch die Auflösung der Anwendungen (Protokoll und Destination-Port) werden bestimmte Mißstände auf den ersten Blick ersichtlich :

A) Backup zur falschen Zeit

In folgendem Fall wurde schon mit der ersten Intraday-Analyse offensichtlich, dass Backups, die laut Planung nur in der Nacht laufen sollten, auch über den Tag verteilt stattfanden :

Intraday Analyse

Alle Protokolle werden angezeigt.
Es werden alle TOS Werte angezeigt.
10.08.2004 00:00 - 23:55



Protokoll	Byte	%
Omniback	155.18 GB	43.79
NCP	122.36 GB	34.53
rtp-audio	14.66 GB	4.14
NETBIOS-SSN	11.65 GB	3.29
PORT_3396	7.18 GB	2.03
MICROSOFT-DS	5.89 GB	1.66



WWW-HTTP	5.52 GB	1.56
DOMINO	4.95 GB	1.40
PORT_6061	4.61 GB	1.30
PRINTER	4.40 GB	1.24
TELNET	4.21 GB	1.19
HTTP-PROXY	3.94 GB	1.11
SNMP	1.51 GB	0.43
FTP-DATA	1.41 GB	0.40
MPTN	1.38 GB	0.39
X11	1012.39 MB	0.28
SMTP	810.93 MB	0.22
IPSEC_O_TCP	351.66 MB	0.10
DDM-RDB	312.48 MB	0.09
UDP-OTHER	284.75 MB	0.08
NETBIOS-DGM	212.70 MB	0.06
MS-SQL	184.30 MB	0.05
ICMP	181.24 MB	0.05
HTTPS	150.45 MB	0.04
IPX	89.19 MB	0.02
Summe	352.36 GB	99.43
rest		
Summe (rest)	2.01 GB	0.57

Über die Top Session Analyse konnten die verantwortlichen Server sofort bestimmt werden :

Top Sessions

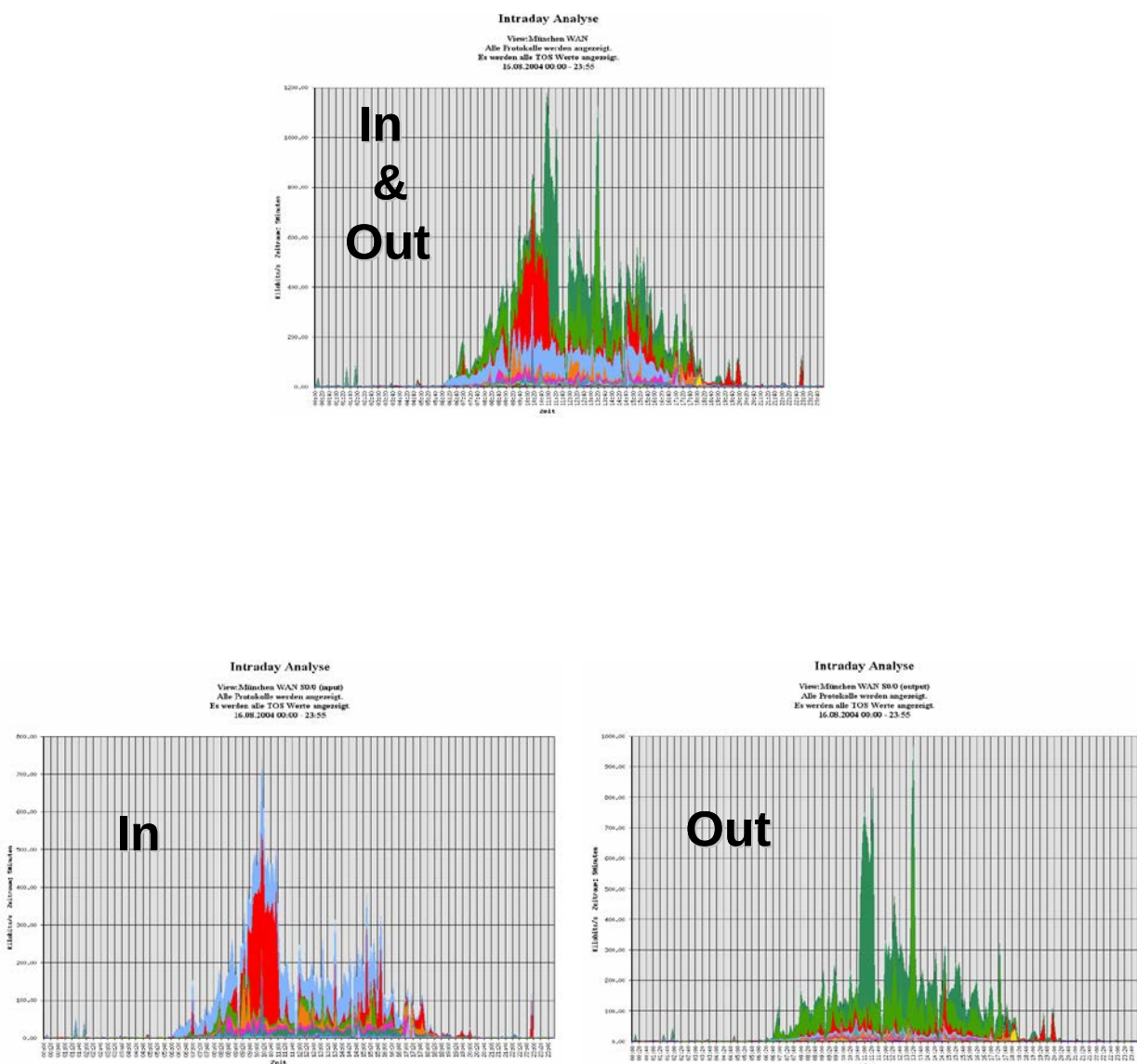
Dargestelltes Protokoll: Omniback.tcp.57120
2.07.2004 11:00 - 22:55

<u>Nr.</u>	<u>Source</u>	<u>Destination</u>	<u>Protokoll</u>	<u>Byte</u>
1	10.1.40.31	<u>10.1.41.67</u>	OMNIBACK.tcp.57120	28.82 GB
2	10.1.40.32	<u>10.1.41.67</u>	OMNIBACK.tcp.57120	9.60 GB
3	<u>10.1.41.67</u>	<u>10.1.40.31</u>	OMNIBACK.tcp. 57120	1.12 GB
4	10.1.41.67	<u>10.1.40.32</u>	OMNIBACK.tcp. 57120	447.44 MB
5	<u>130.50.41.3</u>	<u>10.1.40.43</u>	OMNIBACK.tcp. 57120	42.47 KB
Summe				39.98 GB



B) Asynchrones Routing

Durch die plakative, farbliche Auflösung der Anwendungen (frei definierbar) wurde auch in diesem Fall der Administrator auf einer fehlerhaften Situation aufmerksam, bevor es zu Problemen kam. Auffällig war, dass bestimmte Anwendungen nur in die eine oder andere Richtung auftraten. Ein Blick auf die Router-Konfiguration brachte Fehler im Routing zutage, dass durch die laufende Phase einer Migration von einem Provider zu einem anderen ausgelöst wurde. Während eine Richtung bereits über die neuen Router lief, ging der Rückweg noch über die alte Infrastruktur.



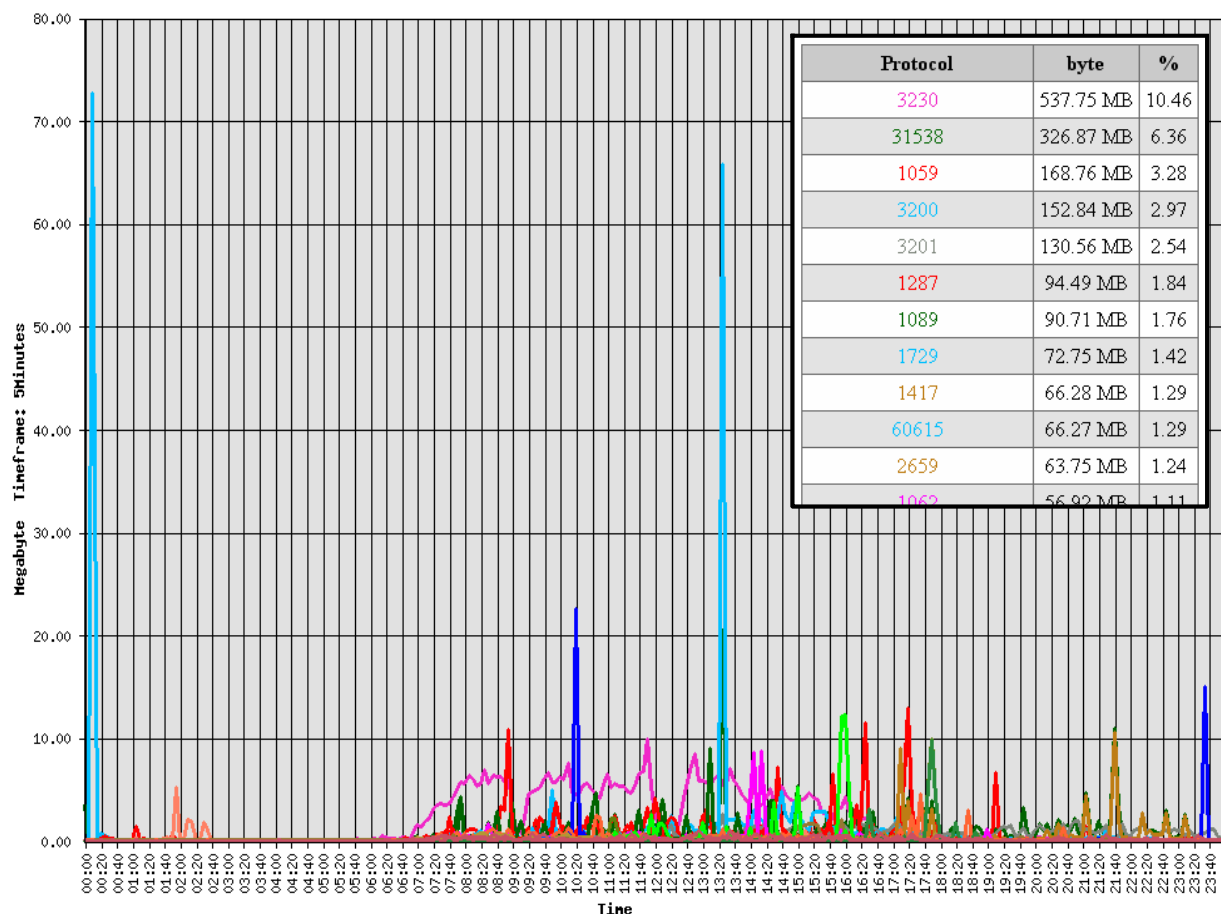


Anwendungsfall #3 – Proprietäre Ports im Netz

IsarFlow benutzt die IANA Definitionen der well-known Ports und well-known Protokolle. Alle Zielports < 1.024 werden automatisch aufgelöst. Alles Ports > 1.024 werden proprietär im Netz verwendet und fallen daher zunächst in die beiden Kategorien TCP- und UDP-Other.

IsarFlow bietet die Analyse ‚unbekannte Ports‘ in welcher der Verkehrs aller Ports, die in die Default-Klassen TCP- oder UDP-Other fallen, aufgeführt werden. Zum Einen wird durch der Customizing-Prozess erleichtert, zum Anderen kann diese Auswertung hilfreich sein, wenn auf einmal der Anteil an „unbekanntem“ Verkehr ansteigt.

Beispielsweise könnte der rollout einer neuen Anwendung im Netz stattgefunden haben, eventuell werden file-sharing Tools mit wechselnden Ports verwendet, oder Viren/Würmer auf neuen Ports tauchen auf.



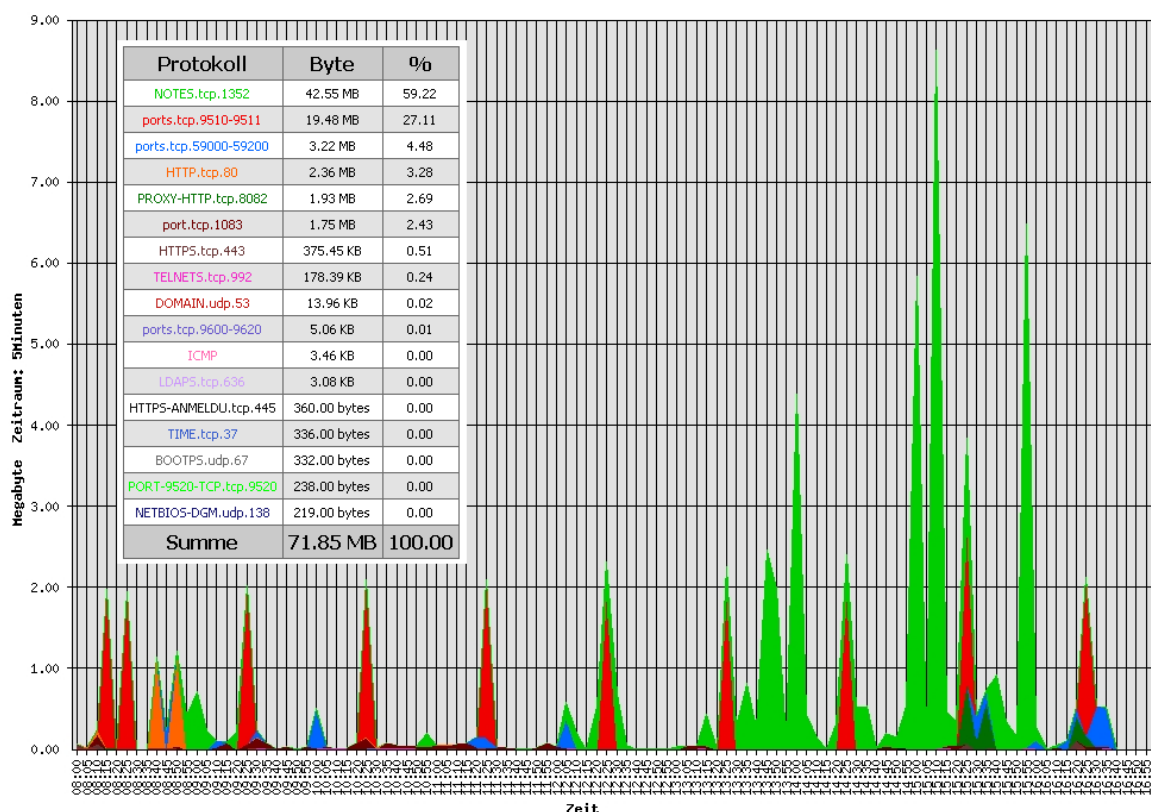


Anwendungsfall #4 – IP Adress Tracking

IsarFlow erlaubt die gezielte Suche nach Anwendungen oder Kommunikationspartnern einer einzelnen IP-Adresse in einem frei wählbarem Zeitraum. Quell- und Ziel-Eingaben dieser Suche können sein : IP-Adresse / Subnet / Any

IPTracking (Protokoll)

IP-2-IP: 192.168.5.11 - any
25.04.2005 08:00 - 17:00
(Intervall 5 min)



IP-Tracking Analyse

IP-2-IP: 192.168.5.11 - any
25.04.2005 15:25 - 15:30

CSV Export

Nr.	Zeit	Source	Destination	Protokoll	Byte	Prozent des gesamten Traffic!
1	15:25:00	172.16.1.117	192.168.5.11	HTTPS.tcp.443	68.79 KB	0.28
2	15:25:00	172.16.16.28	192.168.5.11	ICMP	1.46 KB	0.01
3	15:25:00	172.16.16.29	192.168.5.11	HTTP.tcp.80	768.00 B	0.00
4	15:25:00	172.16.252.1	192.168.5.11	PROXY-HTTP.tcp.8082	756.73 KB	3.03
5	15:25:00	172.16.252.151	192.168.5.11	PROXY-HTTP.tcp.8082	4.39 KB	0.02
6	15:25:00	172.17.1.2	192.168.5.11	ports.tcp.9510-9511	1.95 MB	7.97
7	15:25:00	172.17.1.2	192.168.5.11	DOMAIN.udp.53	2.44 KB	0.01
8	15:25:00	172.17.1.2	192.168.5.11	HTTPS-ANMELDU.tcp.445	120.00 B	0.00
9	15:25:00	172.17.1.2	192.168.5.11	ICMP	60.00 B	0.00
10	15:25:00	172.17.1.21	192.168.5.11	NOTES.tcp.1352	1.08 MB	4.44
11	15:30:00	172.16.252.1	192.168.5.11	PROXY-HTTP.tcp.8082	129.14 KB	0.52
12	15:30:00	172.17.1.9	192.168.5.11	ports.tcp.59000-59200	286.86 KB	1.15
13	15:30:00	172.17.1.21	192.168.5.11	NOTES.tcp.1352	70.00 B	0.00
Summe					4.25 MB	17.41
Gesamter Traffic					24.41 MB	100%



IsarNet
Software Solutions GmbH
Terminalstrasse Mitte 18
85356 München

Tel. 07000 ISARNET
Fax. 089 97007 200
e-mail: isarflow@isarnet.de
<http://www.isarnet.de>
<http://www.isarflow.de>